Hearing before the
Senate Judiciary Committee
Subcommittee on Technology, Terrorism and Government Information

February 1, 2000

Statement of
John S. Tritak
Director
Critical Infrastructure Assurance Office

Mr. Chairman, Madame Ranking Member, members of the Subcommittee, ladies and gentlemen, it is an honor to appear before you here today to discuss the challenges facing our Nation in the area of critical infrastructure protectionthe National Plan for Information Systems Security, Version 1.0. This Subcommittee has shown exceptional leadership on these issues for many years, and I am grateful for the opportunity to work closely with you and the Congress to find ways to advance infrastructure assurance for all Americans. We all recognize that no viable solutions will be discovered or implemented without the executive and legislative branches working together for our national good.

I. Introduction

Mr. Chairman, Madame Ranking Member, members of the Subcommittee, ladies and gentlemen, it is an honor to appear before you here today to discuss with you about the National Plan for Information Systems SecurityProtection, Version 1.0. This Subcommittee has shown exceptional leadership on the matter of critical infrastructure assurance. these issues, and I am grateful for the opportunity to discuss the Administration's efforts to achieve President Clinton's goal of establishing a full operational capability to defend the critical infrastructures of the United States by 2003 against deliberate attacks aimed at significantly disrupting the delivery of services vital to our nation's defense, economic security, and the health and safety of its people. This cannot be done without the support and participation of the Congress.work closely with you and the Congress to find ways to advance infrastructure assurance for all Americans. We all recognize that no viable solutions will be discovered or implemented without the executive and legislative branches working together for our national good.

I. Introduction

When last here in October, I mentioned that America has long depended on a complex of systems B or critical infrastructures B to assure the delivery of services vital to its national defense, economic prosperity, and social well-being. These infrastructures include telecommunications, electric power, oil and gas delivery and storage, banking and finance, transportation, and vital human and government services.

The Information Age has fundamentally altered the nature and extent of our dependency on these infrastructures. Increasingly, our Government, economy, and society are being connected into an ever expanding and interdependent digital nervous system of computers and information systems. With this interdependence comescomes new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in the world can potentially break into sensitive Government files, shut down an airport's air traffic control system, or disrupt 911 services for an entire community.

The threats posed to our critical infrastructures by hackers, terrorists, criminal organizations and foreign Governments are real and growing. President Clinton has increased funding on critical infrastructure substantially overduring the past three years, including a 16% increase in the FY2001 budget proposal to $2.03 billion. He has also developed and funded new initiatives to defend the nation's computer systems from cyber attack. Moreover, to jumpstart the FY01 program initiatives, the President will propose a $9 million supplemental appropriation this spring.

In the 18 months since the President signed Presidential Decision Directive 63, we have made significant progress in protecting our critical infrastructures. In response to the President's call for a national plan to serve as a blueprint for establishing a critical infrastructure protection (CIP) capability, These are issues of the present, not of the future. the National Plan for Information Systems Protection was released last month. It represents the first attempt by any national governmentGovernment to design a way to protect those infrastructures essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and controlled bythrough the use of computers and computer networks.
The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal governmentGovernment to protect the nNation's critical cyber-based infrastructures. Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community.

LaterSubsequent versions will also reflect the interests and concerns expressed by Congress and the general public. That is why the Plan is designated Version 1.0 and subtitled An Invitation to a Dialogue -- to indicate that it is still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment.
Last month the President unveiled our plan, the first of its kind anywhere, for protecting our critical information systems from these threats. It's title, The National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue, is telling. This plan focuses on information systems and primarily on the federal government. Protecting information systems from attacks is a new and extremely complex effort. It is vital to our national security, economic vitality, and public health and safety. And it is, fundamentally and importantly, an effort whose success depends on the ability of the public and private sectors to forge bonds of respect and trust so that we as a nation can work in partnership to undertake the efforts needed to secure our infrastructures. The Plan is about Information sSystem protection, as B a a field of endeavor, is far less mature than that of protecting our infrastructures from physical attacks. However, plans to protect our critical infrastructures from physical attacks are under development, and future versions of the pPlan will include these aspects as well.

Having mentioned the criticality of public-private partnerships, you may note that the Plan's focus is on the federal government B this should not be misunderstood. This focus of this first version of the Plan was necessary to ensure that the federal government would become a model for the nation, in keeping with the President's mandate in PDD-63. However, many efforts are underway to build the critical public-private partnerships needed to successfully defend our nation's information systems. At the release ceremony for the Plan, the President said that "This may be the first time that our Armed Forces alone can not defend our country against potential future enemies. Defense of our cyber space, of the national information infrastructure, requires a public-private partnership." This is, indeed fundamental, and I will address this in some detail shortly.

Finally, as stated in the title of the Plan, this is indeed Version 1.0, and truly is an invitation to a dialogue B a dialogue with the private sector, with state and local governments, and with the Congress. We are confident that this dialogue will go a long way towards forging the bonds of trust and respect between all parties on this new and important effort and in furthering CRITICAL INFRASTRUCTURE PROTECTIONcritical infrastructure protection.

II. The Plan: Overview and HighlightsStructure of the Effort

President Clinton directed the development of this Plan to chart the way toward the attainment of a national capability to defend our critical infrastructures by the end of 2003. To meet this ambitious goal, the Plan establishes ten10 programs for achieving three broad objectives. They are:

Objective 1: Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

Program One1 calls for the GovernmentGovernment and the private sector willto identify significant assets, interdependencies, and vulnerabilities of critical information networks tofrom attack, thenand to develop and implement realistic programs to remedy the vulnerabilities, while continuously updating the assessment and remediation efforts.

Objective 2: Detect and Respond: Develop the means required to identify and assess attacks in a timely way, contain such attacks, recover quickly from them, and reconstitute those systems affected.

Program Two2 will install multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers will receive warnings from these detection devices, as well as Computer Emergency Response Teams (CERTs) and other means, in order to analyze the attacks, and assist sites in defeating attacks.
Program 3 will develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the Llaw. It will assist, transform, and strengthen U.S. law enforcement and intelligence agenciesAgencies to be able to deal with a new kind of threat and a new kind of criminal --, one that acts against computer networks.

Program 4 calls for a more effective nationwide system to share attack warnings and information in a timely manner, including improved information sharing within the Federal government; encouraging private industry, as well as state and local governments, to create and Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local governments and could receive warning information from the Federal Government; and removing existing legal barriers to information sharing.

Program 4 calls for a more effective nationwide system to share attack- warnings and information in a timely manner. This includes improving information sharing within the Federal governmentGovernment and encouraging private industry, as well as state and local governmentGovernments, to create Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local governmentGovernments, and could receive warning information from the Federal GovernmentGovernment. Program 4 additionally calls for removfor removingal of existing legal barriers to information sharing.

Program 5 will create capabilities for response, reconstitution, and recovery to limit an attack while it is underway and to build into corporate and agencyAgency continuity and recovery plans the ability to deal with information attacks. The goal for GovernmentGovernment and the recommendation for industry is that every critical information system have a responserecovery plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems.

Objective 3: Build Strong Foundations: Take all actions necessary to create and support the Nation's commitment to Prepare and Prevent and to, Detect and Respond to attacks on our critical information networks.

Program 6 will systematically establish research requirements and priorities needed to implement the Plan, ensures their funding, and creates a system to ensure that our information security technology stays abreast with changes in the threat environment. and in overall information systems.

Program Seven7 will survey the numbers of people and the skills required for information security specialists within the Federal GovernmentGovernment and nationwidethe private sector, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program Eight8 will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyberattackcyber-based attacks.

Program Nine9 will develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation betweenwithin the Federal GovernmentGovernment, including Congress, and between the Government and private industry.

Program Ten10 builds mechanisms to highlight and addressprioritize isprivacy issues in the development of each and incorporated in every other program:. Infrastructure assurance goals must be accomplished in a manner that maintains, and even strengthens, American's privacy and civil liberties and is making what we do in the protection of critical cyber systems conform to Constitutional and other legal rights, including ensuring the full protection of American citizens' civil liberties, their Rights to privacy, and their rights to the protection of proprietary data. The Plan outlines nine specific solutions, which include consulting with various communities; focusing on and highlighting the impact of programs on personal information; committing to fair information practices and other solutions developed by various working groups in multiple industries; and working closely with Congress to ensure that each program meets standards established in existing Congressional protections.

* * *

I would like to highlight a few of these programs in the remainder of my testimony. In these These programs, the Administration seeks to accomplish two broad aims of the Plan B the establishment of the U.S. governmentGovernment as a model of information securityinfrastructure protection, and the development of a public-private partnership to defend our national infrastructures.

A. The Federal GovernmentGovernment as a Model of Information Security

In speaking of the Plan, I will address many aspects of our critical infrastructure protection efforts, both current and planned, and endeavor to give you as complete a picture as I can in this brief time. There are many ways to address this. The plan is written programmatically, and addresses three fundamental categories, Prepare and Prevent, Detect and Respond, and Build Strong Foundations. These are further broken further down into ten programs, detailed in the attached Executive Summary. A second paradigm considers two primary foci B Government as a Model and Public-Private Partnership.

Both paradigms share the fundamental bedrock princritical infrastructure protectionleprinciple of absolute respect for and preservation of the privacy rights and civil liberties of Americans and our CConstitutional form of government. This fundamental responsibility of good governance has two aspects. First, do no harm B undertake no effort that in any way detracts from the rights and liberties of us all. This is reflected in all programs in the Plan, and is highlightedbut especially in Program 10, which is specifically dedicated to this critical areathe full protection of American citizens' civil liberties, their rights to privacy, and their rights to the protection of proprietary data. ThisDoing no harm, however, is the simple part. The second aspect is to hold safe and confidential the data given to the Government by all Americans. IRS records, Medicare and Medicaid files, and worker and veteran compensation and veteran records are but a few examples. This challenge is fundamentally one of information security B of assuring that no one of malicious intent can break theinto government information systems and read or copy our personal information. The government also holds information shared with it by business on a confidential basis. This, too, must be held safe from intruders to help assure our economic viability and vitality. This second aspect, securing our information systems, is a fundamental challenge of our information technology age, and requires information technology solutions. TI will talk to our proposed solutions shortly, and these concerns are addressed in the Plan.

As the Plan and its Executive Summary are laid out programmatically and are available to you, I will focus on this second paradigm of Government as a Model and Public-Private Partnership. Finally, although a portion of the Plan is dedicated to Defense CRITICAL INFRASTRUCTURE PROTECTIONcritical information protection efforts, I will not address these here. Rather I refer you to the Department of Defense for a thorough explanation of their efforts. shortly uFramework of the Effort

Let me first emphasize to you that the threat to our infrastructures from hackers, terrorists, criminal organizations and foreign governments is real. This will be addressed shortly, and in as much detail as is allowable in open forum, by Mike Vatis, so I will not dwell on them here. Instead I want to paint for you the framework for our efforts and our plans.

A. Historical Background

Allow me first to address briefly the origins of Presidential Decision Directive 63 (PDD 63), which sets forth the Administration's critical infrastructure assurance policy and implementation guidance. Our national defense, economic prosperity, and quality of life have long depended on the essential services delivered by critical infrastructures B including energy, banking and finance, transportation, telecommunications, and certain vital human services, such as fire protection and emergency medical services. The 1995 bombing of the Murrah Federal Building in Oklahoma City aptly demonstrated that these critical infrastructures are highly vulnerable to new types of threats and vulnerabilities B many of which this nation is unprepared to defend against.

In response to this tragedy, the Administration formed an inter-agency working group to examine the nature of the threat, our infrastructure vulnerabilities, and possible long-term solutions for this aspect of our national security. The Critical Infrastructure Working Group (CIWG), chaired by Jamie Gorelick and including representatives from the Defense, Intelligence, and national security communities, identified both physical and cyber threats and recommended formation of a Presidential Commission to address more thoroughly many of these growing concerns.

In July 1996, in response to the CIWG recommendation, President Clinton signed Executive Order 13010 establishing the President's Commission on Critical Infrastructure Protection (PCCIP or, the Commission). After examining thes issues for over a year, the Commission issued its report, Critical Foundations, Protecting America's Infrastructures, drawing at least four significant conclusions:

First, critical infrastructure protection is central to our national defense, including national security and national economic power;

Second, growing complexity and interdependence between critical infrastructures may create increased possibility that rather minor and routine disturbances can cascade into national security emergencies;

Third, vulnerabilities are increasing steadily and that means to exploit weaknesses are readily available; practical measures and mechanisms, the commission argued, must be urgently undertaken before we are confronted with a national crisis; and

Fourth, laying a foundation for security will depend on new forms of cooperation with the private sector, which owns and operates many of these critical infrastructure facilities.

II. PDD 63 - Overview

After releasing the PCCIP report, the Administration worked to incorporate these and other recommendations into Presidential Decision Directive 63, which was issued in May 1998.
Most importantly, PDD 63 recognizes this need for a Public-Private Partnership to face these critical issues. The directive specifies sectors of the national infrastructure, primarily in the private sector, that provide critical services or functions, and designates lead agencies in the federal government to act as Sector Liaisons. PDD 63 additionally recognizes that the traditional areas of national defense, foreign affairs, intelligence, and law enforcement are fundamental to infrastructure protection, are inherently the domain of the government, and stipulates that sector coordinators are to be designated from the associated government agencies to integrate these efforts in a coordinated national program.

PDD 63 established the position of National Coordinator for Security, Infrastructure Protection, and Counter Terrorism to orchestrate these efforts. The PDD lays out specific tasks that must be accomplished, time lines for doing so, and organizations for carrying out these missions. Key amongst them are the National Infrastructure Protection Center (NIPC), Directed by Mike Vatis, and the National Plan Coordinating Staff B now called the Critical Infrastructure Assurance Office (CIAO) B which I have the honor of directing.

PDD 63 focuses the nation's efforts on aspects of critical and immediate importance -- and I emphasize that these must be the efforts of the whole nation, for success will come only from the efforts of the private sector, state and local governments, and the federal government working together in an integrated and cooperative manner. Our efforts fall in three broad categories.

A. National Security Component

The first is the federal government agencies involved in National Security B primarily DoD and the Intelligence Community. The armed forces and associated agencies have requirements and systems that are unique to their special role. This has long been recognized in law, in the way we structure these organizations, and in our national philosophy. Their efforts are, as would be expected from the sensitive and well established nature of their mission, much further along in achieving Critical Infrastructure Protection than those of the other parts of the federal government. In many ways they have set the example for other agencies' efforts, and they currently share their experiences and advise on how the rest of the government might proceed. Their contribution has been very important in shaping the policy and programmatic reality the rest of the government is currently trying to establish. Mr. Richard Schaeffer, Director of the Information and Infrastructure Assurance Office for the Defense Department, has submitted a statement for the record on this and other matters, so, in cause of brevity, I will refer you to it and cover their efforts no further.

BA. Government as Model

The second category of effort can be called "Government as a Model." We often say that more than 90% of our critical infrastructures are neither owned nor operated by the federal governmentFederal Government. Partnerships with the private sector and State state and Llocal Governmentgovernments are therefore not just needed, but are the fundamental aspect of critical infrastructure protection. Yet, the President rightly challenged the federal

governmentFederal Government in PDD-63 to serve as a model for Critical critical Infrastructure infrastructure Protection protection B to put our own house in order first. To this end, the President has developed and provided full or pilot funding for the following key initiatives designed to protect the federal governmentGovernment's computer systems:As such, we the Administration hashave focused what might appear to be a disproportionate amount of our effort early in the process on doing this by establishing a coordinated and integrated approach across the federal governmentFederal Government. Let me outline the major initiatives in this area for you.

1. Federal Computer Security Requirements and GovernmentGovernment Infrastructure Dependencies.

One component of this effort supports aggressive, governmentGovernment-wide implementation of federal computer security requirements and analysis of vulnerabilities. Thus, in support of the release ofsupport of PDD 63 the National Plan, the PresidentPresident announced his intent to create a permanent Expert Review Team (ERT) at Bill Clinton has forwarded to Congress a requests for a FY 2000 budget amendment that would enhance computer security and critical infrastructure protection in the Federal Government. This proposal would fund a permanent 15-member team at the Department of Commerce's National Institute of Standards and Technology (NIST). The ERT will be responsible for helping AgenciesAgencies identify vulnerabilities, plan secure systems, and implement Critical Infrastructure Protection Plans. The remaining $3 million will establish an operational fund at NIST for computer security projects among Federal Agencies, including independent vulnerability assessments, computer intrusion drills, and emergency funds to cover security fixes for systems identified to have unacceptable security risks. The Pursuant to existing Congressional authorities and administrative requirements, the Director of the ERT team would consult with the Office of Management and Budget and the National Security Council on the team's plan to protect and enhance computer security for Federal AgenciesAgencies. The President's Budget for FY2001 will propose $5 million for the ERT.

2. Critical Infrastructures B National Security Interdependencies and Planning

Under PDD-63, the President directed the The Administration, in marshaling resources to implement PDD-63, requires the CIAO to examine the complex national security interdependencies of critical infrastructure nodes and systems:

"The [CIAO] will Y to coordinate analyses of the U.S. Government's own dependencies on critical infrastructures."

An additional component is to identify critical infrastructure dependencies. Many of the critical infrastructures that support our nation's defense and security are shared by multiple agenciesAgencies. Even within governmentGovernment, then, critical infrastructure outages may cascade and unduly impair delivery of critical services. The CIAO is coordinating an interagency effort to We must develop a more sophisticated identification of critical nodes and systems, and to understand their impact on national defense and security, national economic security, and public health and safety governmentGovernment-wide. These efforts will support the work of the ERT in identifying vulnerabilities of the governmentGovernment's informationcomputer infrastructures, and provide valuable input to agenciesAgencies for planning secure computer systems, and implementing computer security plans. These PDD-63 stipulates that these particular efforts B to assist government agencies in analyzing their vulnerabilities B be are managed by the Critical Infrastructure Assurance Office. This exciting research, when complete, will providepermit the Federal Government to identify and redress its most significant critical infrastructure vulnerabilities first, and provide the necessary framework for well informed critical infrastructure protection policy making and budget decisions important information to maximize national security research and development, budgeting, and for implementing computer security requirements and critical infrastructure planning within each agency.

Federal Intrusion Detection Network (FIDNet).

PDD-63 marshals Federal Government resources to improve interagency cooperation in detecting and responding to significant computer intrusions into civilian Government critical infrastructure nodes. The program B much like a

centralized burglar alarm system B would operate within long-standing, well-established legal requirements and Government policies covering privacy and civil liberties. Contrary to erroneous news reports in the past, private entities will not be wired into FIDNet, and the FBI will not run it. I cannot over-emphasize the point, that FIDNet is intended to protect information on Government computers, including that of private citizens (e.g. tax returns), and not invade the privacy or violate the rights of Americans.

To support this effort, the Administration will propose funding in the President's FY2001 Budget ($10 million) to create a centralized intrusion detection and response capability in the General Services Administration (GSA). This capability will assist Federal Agencies to:
detect and analyze computer attacks and unauthorized intrusions;
share attack warnings and related information across Agencies; and
respond to attacks in accordance with existing procedures and mechanisms.
FIDNet is intended to promote confidence in users of Federal civilian computer systems. It is important to recognize that FIDNet has a graduated system for response and reporting, Attack and intrusion information would be gathered and analyzed by home-Agency experts. Only data on system anomalies would be forwarded to GSA for further analysis. Thus, intrusion detection would not become a pass-through for all information to the Federal Bureau of Investigation or other law enforcement entities. Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules B no new authorities are implied or envisioned by the FIDNet program.

One additional benefit of Government-wide intrusion detection is to improve computer intrusion reporting. Various authorities require Agencies to report criminal intrusions to appropriate law enforcement personnel, which include the National Infrastructure Protection Center. FIDNet will support law enforcement's responsibilities where cyber attacks are of a criminal nature or threaten national security.

In short, FIDNet will

be run by the GSA, not the FBI;
not monitor any private networks or email traffic;
confer no new authorities on any Government Agency; and
be fully consistent with privacy law and practice.
--Byies Neither the ,-- exceptonlyrenAlso,

Ppin

Education and Training

Federal Cyber Services (FCS). One of the nation's strategic shortcomings in protecting our critical infrastructures is a shortage of skilled information technology (IT) personnel. Within IT, the subsethortage of information systems security personnel, the shortage is acute, and. tThe Federal Government's shortfall of skilled information systems security personnel amounts to a crisis. This shortfall reflects a scarcity of university graduate and undergraduate information security programs and the inability of the governmentGovernment to provide the salary and benefit packages necessary to compete with the private sector for these highly skilled workers. In attacking this problem through the Federal Cyber Services (FCS) initiative described below, we willare leverageing the initial efforts made by the Defense Department, National Security Agency, and some other Federal Agencies. The President's Budget for FY2001 will propose $25 million for this effort.

The Federal Cyber Services (FCS) training and education initiative, highlighted by the President at the Plan's release, introduces five programs to help solve the Federal IT security personnel problem.

A study by the Office of Personnel Management to identify and develop competencies for federal information technology (IT) security positions, and the associated training and certification requirements.

The development of Centers of IT Excellence to establish competencies and certify current Federal IT workers and maintain their information security skill levels throughout their careers.

The creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT managers by awarding scholarships for the study of information security, in return for a commitment to work for a specified time for the federal Government. This program will also support the development of information security faculty.

The development of a high school recruitment and training initiative to identify promising high school students for participation in summer work and internship programs that would lead to certification to Federal IT workforce standards and possible future employment.

The development and implementation of a Federal INFOSEC awareness curriculum aimed at ensuring computer security literacy throughout the entire Federal workforce.

Research and Development.

A key component to our ability to protect our critical infrastructures now and in the future is a robust research and development plan. T As part of the structure established by PDD-63, the interagency Critical Infrastructure Coordination Group (CICG) has created a process to identify technology requirements in support of the Plan. Chaired by the Office of Science and Technology Policy (OSTP), the Research and Development Sub-Group works with Agencies and the private sector to:

gain agreement on requirements and priorities for information security research and development;

coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts;

communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia; and

identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

That process, begun in 1998, led tohas helped focus efforts on coordinated cross-governmentGovernment the Administration budget request for FY2000 of $500M for critical infrastructure protection research. Among the priorities identified by the process are:

technology to support large-scale networks of intrusion detection monitors;

artificial intelligence and other methods to identify malicious code (trap doors) in operating system code;

methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster;

technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as the critical infrastructures themselves; and

technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.

The President's Budget for FY2001 will propose $621 million across all Agencies for critical infrastructure related R&D investment.

The need exists, however, to coordinate R&D efforts not just across the federal governmentGovernment, but between the public and private sectors as well. A fundamentally important initiative that has the ability to pull disparate pieces of the national R&D community into closer relationships is the Institute for Information Infrastructure Protection (I3P),

and organization created to identify and fund research and technology development to protect America's cyberspace from attack or other failures. I will discuss this in detail when I address Public-Private Partnership issues.

Public Key Infrastructure.

Protecting critical infrastructures in the Federal Government and private sectors requires development of an interoperable public key infrastructure (PKI). A PKI enables data integrity, user identification and authentication, user non-repudiation, and data confidentiality through public key cryptography by distributing digital certificates (essentially electronic credentials) containing public keys, in a secure, scalable, and reliable manner. The potential of PKI has inspired numerous projects and pilots throughout the Federal Government and private sectors. The Federal Government has actively promoted the development of PKI technology and has developed a strategy to integrate these efforts into a fully functional Federal PKI. The President's Budget for FY2001 will propose $7 million to ensure development of an interoperable Federal PKI.

To achieve the goal of an integrated Federal PKI, and protect our critical infrastructures, the Federal Government is working with industry to implement the following program of activities:

Connect Agency-wide PKIs into a Federal PKI: DoD, NASA, and other Government Agencies, are actively implementing Agency-wide PKIs to protect their internal critical infrastructures. While a positive step, these isolated PKIs do not protect infrastructures that cross Agency boundaries. Full protection requires an integrated, fully functional PKI.

Connect the Federal PKI with Private Sector PKIs: Private sector groups are actively developing their own PKIs as well. While a positive step, these isolated PKIs do not protect infrastructures that cross Government or industry sector boundaries.

Encouraging development of interoperable Commercial Off-the-Shelf PKI Products: Limitation to a single vendor's solution can be a serious impediment, as most organizations have a heterogeneous computing environment. Consumers must be able to choose COTS PKI components that suit their needs.

Validating the Security of Critical PKI Components: Protecting critical infrastructures require sound implementation. The strength of the security services provided to the critical infrastructures depends upon the security of the PKI components. Validation of the security of PKI components is needed to ensure that critical infrastructures are adequately protected. NIST is pursuing a validation program for PKI components.

Encouraging Development of PKI-Aware Applications: To encourage development of PKI-aware applications, the Government is working with vendors in key application areas. One example is the secure electronic mail projects that have been performed jointly with industry.Aspect of a Public Key Infrastructure (PKI) are currently ubiquitous on the web B the ability to use encryption to send your credit card number securely to an on-line vendor is the most common. Yet this is just one aspect. PKI is another complicated and important aspect of information security that needs to be addressed. The Treasury Department is leading the Administrations efforts to develop PKI programs to fill information security needs, and this effort was highlighted at the release of the National Plan. It is important to note that PKI, through its enabling of the wide-spread use of encryption technology, will assure some fundamental characteristics of electronic communications. Key among these for information systems protection is the characteristic of non-repudiation B that is, the content and identity of the sender of information, and possibly the originator of all actions on the web, is not reputable. With this in mind, a couple of fundamental issues, both current and future, are worth mentioning.

On On the current side, malicious activities in information systems are in large part made possible by the anonymity of their perpetrators on the web. PKI, where implemented, has the ability to fix an identity to the users of information systems. Without the assumption of anonymity, malicious actions on the web and in information systems would much more strongly resemble traditional "physical" malicious actions in other spheres. This may give pause to would-be perpetrators, just as it does to those who would perform malicious physical acts, and give law enforcement tools to more easily apprehend those who break the law.

In the near future, information systems will go through revolutionary change with the advent of the Next Generation Internet (NGI). Just as the Internet fundamentally and quickly changed the way we do business, and introduced the very problems that we are here today discussing, the NGI will make many things, both constructive and destructive, possible that here-to-fore were not. PKI security paradigms in these soon-to-be information systems may be a key component in dealing with security problems.

The Institute will fill research and other key technical gaps that neither the private sector nor the government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure.

The President announced he would propose initial funding of over $50 million for the Institute in his budget to be submitted this month. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST).

The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and the supported by leading corporate Chief Technology Officers (CTOs).

The Institute will work directly with private sector information technology suppliers and consumers to define research priorities and engage the country's finest technical experts to address the priorities identified. Research work will be performed at existing institutions including private corporations, universities, and non-profit research institutes. The Institute will also make provisions for private sector funding for some research activities.

CB. Public-Private Partnership

The security of information flowing over the information highway is a critical element of E-commerce, as well as to our national security. It is a necessary part of building trust in the accuracy and integrity of transactions made over the information infrastructure. There is a growing awareness that America's information infrastructure B the basis of E-Commerce B is becoming an increasingly attractive target for deliberate attack or sabotage. A strategy of cooperation and partnership between the private sector and the U.S. governmentGovernment to protect the nation's infrastructure is the linchpin of this effort. The President is committed to building partnerships with the private sector to protect our computer networks through the following initiatives:

Institute for Information Infrastructure Protection (I3P). The Institute would identify and address serious R&D gaps that neither the private sector nor the governmentGovernment's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. The President announced he would propose initial funding of over $50 million for the Institute in his FY 2001FY2001 Budget. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this independent organization. The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and the supported by leading corporate Chief Technology Officers.

The Institute will work directly with private sector information technology suppliers and consumers to define research priorities and engage the country's finest technical experts to address the priorities identified. Research work will be performed at existing institutions including private corporations, universities, and non-profit research institutes. The Institute will also make provisions for private sector funding for some research activities.

Partnership for Critical Infrastructure Security. Last December, Secretary Daley met with senior representatives from over 90 major corporations, most Fortune 500, representing owners and operators of critical infrastructures, their suppliers, and their customers, to discuss the building a Partnership for Critical Infrastructure Security. Industry has taken the lead on this effort, and organized a meeting at the U.S. Chamber of Commerce for later this month to give substance and purpose to the Partnership.

The Partnership will explore ways in which industry and governmentGovernment can work together to address the

risks to the nation's critical infrastructures. Federal Lead AgenciesAgencies are currently building partnerships with individual infrastructure sectors in private industry, including communications, banking and finance, transportation, and energy. The Partnership will serve as a forum in which to draw these individual efforts together to facilitate a dialogue on cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership hopes to raise awareness and understanding of, and to serve, when appropriate, as a catalyst for action among, the owners and operators of critical infrastructures, the risk management and investment communities, other members of the business community, and state and local governmentGovernments.

National Infrastructure Assurance Council (NIAC). President Clinton established the NIAC by Executive Order 13130 on July 14, 1999. When fully constituted, it will consist of up to 30 leaders in industry, academia, the privacy community, and state and local governmentGovernment. The NIAC will provide advise and counsel to the President on a range of policy matters relating to critical infrastructure assurance, including the enhancement of public-private partnerships, generally. Thirdly, and aAs discussed abovehighlighted by the President on January 7th, one of thea most important components of PDD 63PDD-63 implementationof critical infrastructure protection is the developing partnership between the Private private Sectorsector, State state and Local local Governmentsgovernments, and the Federal GovernmentFederal Government. The importance of this effort cannot be overstated and is made clear by considering just a few scenarios. If the natural gas delivery system you rely on for heat and cooking fails in Januaryduring a snow storm, due to an attack on the computer systems that direct its operations, you will take small comfort in fact that the federal governmentFederal GovernmentCommerce department has a first class Ccritical iInfrastructure pProtection to protect its in-house critical systemsoperation. In fact, all our efforts toIf we succeed in put theprotecting federal Federal government's Government's information systems, house in order and to serve as a model for industry will be of little service if our government information systems are impossible to break into, butbut the electrical power upon which they dependthat they operate on is shut down by malicious actions of a foreign government, critical services will be denied. Or if the telecommunications system in a major metropolitan area is brought down by international terrorists, interrupting 911 service, e-commerce, e-banking, and countless other services, the fact that the Federal Government published a Plan for Information Systems Security will mean nothing. The list of examples goes can go on and on, and none of these systems is owned or operated by the federal governmentFederal Government.

These vignettes put the situation in perspective B we are faced with a fascinating and challenging problem. This is the first time that I am aware of in our national history that by creating policy and expending resources, the federal governmentFederal Government cannot alone solve a national security problem. So what are we doing about it? If by "we" you understand "the government" then the answer must necessarily be unsatisfactory B because the government alone cannot do enoughcannot protect the nation's infrastructures.. But if by "we" you understand "the nation" B the federal governmentFederal Government in a coordinated and integrated effort with state and local government, industry, academia and other concerned groups B then I am happy to report that we have made a good beginning, and are developing a strong future.

Just last FridayLast October, Treasury Secretary Summers announced the formation of the Financial Sector Information Sharing and Analysis Center B "ISAC" for short. Telecommunications has had the NCC fulfilling the role of its ISAC long before the government recognized that this concept would be needed on a broader base. ISACs are private sector owned and operated entities that serve as focal points for their associated sectors of the economy. Because they are defined individually by their member organizations, they will not all be identical. They are, however, all envisioned to be the coordinating and analyzing body for cyber attacks on their specific sector. I want to emphasize that these ISACs are neither set up, not nor supervised by the federal governmentFederal Government, although . Tthe federal governmentFederal Government will assist, these critical sectors in setting up their ISAC, through the Sector LiaisonsLead agencies, if asked. The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism has also pledged that the government will share what information we can on cyber attacks with the ISACs, to help them protect their sector, and. W we will also encourage them to share appropriately sanitized information with us government to help us protect government agencies and functions. But this sharing from ISACs to government will be on an entirely voluntary basis, both in amount of information and the level of detail. No requirement exists or will exist that mandates demand they share information sharing.

While these ISACs, would work within the sectors of the economy that own and operate critical infrastructure, as stipulated in PDD-63, this is not intended to be limiting. Other sectors or groupings within industry could establish

ISACs, and we would assist them in this. Furthermore, practically every aspect of our nation relies on critical infrastructures. This makes CIPCRITICAL INFRASTRUCTURE PROTECTIONmakes critical infrastructure protection a fundamentally important issue for not just those companies that own and operate critical infrastructure, but also for those that rely on it to do business B their consumers. They can and must have a voice in this public/private partnership. Two bodies that help facilitate partnership not only with the owners and operators, but with corporate consumers as well, are of particular note.

RecentlyLast summeratheAdditionally, as stipulated in PDD-63, the President will soon announce the formation of the National Infrastructure Assurance Council (NIAC). This Presidential advisory body will have representatives from the Private Sector, State and Local gGovernments, and the Federal Government. It will examine key aspects of critical infrastructure assurance, act as a focal point for critical issue, and report to the President.

Last December, Secretary Daley met with senior representatives from over 90 major corporations, most Fortune 500, representing owners and operators of critical infrastructures, their suppliers, and their consumers, to discuss the idea of formalizing a partnership. Industry has taken the lead on this effort, and organized a meeting at the U.S. Chamber of Commerce for later this month to give substance to and formalize the Partnership. While the government cannot and does not wish to dictate the form or agenda for the Partnership, I believe this body will take up many cross-cutting issues of widespread importance to industry and government. I want to emphasize that the Partnership must be truly that B a partnership in which all voices are equal, and all concerns are adequately addressed.We are, therefore, working towards establishing two bodies of fundamental interest to this committee.

1. National Infrastructure Assurance Council

The first is the National Infrastructure Assurance Council. Text Y

2. Partnership for Critical Infrastructure Protection

Second is the Partnership for Critical Infrastructure Protection. Text Y

3. State and Local Governments

The final indispensable members of this partnership are State state and Local local Governmentsgovernments. They have the fundamentally important roles of providing and regulating many if not most essential services. They are the front line forces in the event of disasters or attacks on infrastructures. Some have moved quite far in their CIP critical infrastructure protection efforts B New Mexico, for example, under the direction of Dr. Dan O'Neieal, has a very strong and growing CIP critical infrastructure protection partnership with key private sector entities. Furthermore, we have long had strong relationships with state and local governments on specific issues related to critical infrastructure protectionCIP, such as state and local emergency management organizations with FEMA, and state and local law enforcement agencies through the FBI and others national law enforcement agencies. This area is one in which much work remains to be done, and I look forward to working with each Congressional Delegation as we define the issues and solutions.

Finally, as mentioned earlier, the Institute for Information Infrastructure Protection will require the close partnership and efforts of the public and private sectors. It is designed to fill the key R&D and other technical gaps that neither the private sector nor the government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure.

The President announced he would propose initial funding of over $50 million for the Institute in his FY 2001 Budget. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this independent organization.

The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and the supported by leading corporate Chief Technology Officers.

The Institute will work directly with private sector information technology suppliers and consumers to define research priorities and engage the country's finest technical experts to address the priorities identified. Research work will be

performed at existing institutions including private corporations, universities, and non-profit research institutes. The Institute will also make provisions for private sector funding for some research activities.

III. Conclusion

In conclusion, the National Plan is an important step forward. My staff and I are committed to building on this promising beginning, coordinating the Government's efforts into an integrated holistic program for critical infrastructure protection under the directionin support of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and the Federal GovernmentGovernment, generally. We have much work left to do, and I hope to work with the members of this committee, indeed with the Congress as a whole, as we wrestle with this developing field and implement solutions. I look forward to your questions.

III. Critical Infrastructure Assurance Office

Let me change the focus of my statements now from that of a PDD-63 overview, and tell you about the CIAO.

A. Tangible Accomplishments

Our office has been a vigorous one, with a full agenda. Since its inception in May 1998, the Critical Infrastructure Assurance Office has met several important milestones. These include:

Establishing and coordinating the efforts of an Expert Review Team that has analyzed and critiqued the critical infrastructure protection plans of numerous Federal agencies;

Hosting a January 1999 conference to improve information sharing with owners and operators of critical infrastructure facilities;

jointly hosting a Freedom of Information Act (FOIA) workshop with the Department of Justice in July 1999, designed to foster information sharing channels;

Preparing for a national kickoff this fall of the Partnership for Critical Information Security, a national awareness campaign and public-private partnership mandated in PDD-63;

Establishing a program office, in cooperation with the General Services Administration, to support the piloting of the proposed Federal Intrusion Detection Network (FIDNet) initiative;

Assisting in the coordination of an interagency process for developing long-term research and development strategies consistent with PDD-63; and

Laying the groundwork for creation of the National Infrastructure Assurance Council (NIAC)-a Presidential-level advisory committee for critical infrastructure assurance policy making.

The CIAO continues to strive toward the successful completion of the goals set by the President in PDD-63. The first version of the integrated National Plan will be released shortly, and our efforts to assist in the support of infrastructure assurance objectives is ongoing.

B. FY 2000 Priorities

For Fiscal Year 2000, I have four key priorities for the CIAO. These represent activities which serve the Federal Government and our partner organizations such as a the National Infrastructure Protection Center (NIPC) and the Office of the Secretary of Defense (OSD) as a whole, and for which the CIAO is an ideal organization to provide. Most important, these activities do not duplicate the efforts of other government organizations.

1. Partnership: Government B Private Sector

The first priority is laying the foundations for a genuine partnership between the corporate community in America and the Federal Government. My staff has several initiatives underway where we are working closely with industry associations, individual companies and concerned citizens to find ways for government and industry to work together. We are specifically looking at ways of learning from each other's best practices, ways in which we can share information without violating each other's equities, and ways to make the most of new technologies in infrastructure assurance. Throughout this work, my staff and I are very much aware that over 90 percent of the nation's infrastructures are owned and operated by someone other than the Federal Government. I know that there is no way the government can move forward in protecting the nation without help from industry.

2. Partnership: Federal B State & Local Governments

The second priority is to lay the foundations for an equally important partnership between state and local governments and the Federal Government. We plan to work closely with the national associations whose members are governors, mayors, state legislators, and state, county and local officials. We will also be working directly with the elected and appointed state and local officials themselves to include members of the fire service, police, emergency medical services and the emergency management communityand will follow their lead on issues in their jurisdictions. This is important because the bulk of the nation's response assets are the responsibility of the our governors and mayors. State and local governments also have excellent relationships with industry at the local level and we hope to use that positive synergy in our work.

3. Education and Awareness

The third priority is increase the level of education and awareness on infrastructure assurance both within government and industry. A survey taken by the CIO Council in September 1999 on PDD-63 indicated that 45 percent of the respondents had not heard of it. We have much work ahead of us to elevate infrastructure assurance at all levels.

4. Infrastructure Interdependencies - Critical Node Analysis

The fourth priority is to work closely with Federal departments and agencies to conduct a critical node analysis so that individual agencies may better understand where their most important vulnerabilities lie and can make resource decisions accordingly. From our perspective of looking across the entire government, we feel this is a valuable service we can offer our fellow agencies and bring to bear on the problem the full range of expertise to which we have access, and one which we are specifically tasked to do under PDD-63.

All of these activities will all be conducted in parallel, and.W we will use positive lessons learned in from one area to good usefurther our efforts in the other areas.

In addition, the CIAO will be working very closely with the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism on a variety of other initiatives. For example, we will continue to support the activities of the Critical Infrastructure Coordination Group and the newlysoon to be -created National Infrastructure Assurance Council whose members will be appointed by the President.

We will also be working closely the departments and agencies that will be working addressing specific programmatic areas supporting PDD-63 initiatives B such as the Department of the Treasury, the General Services Administration, the National Institute of Standards and Technology and the Office of Personnel Management. We will provide such support as is necessary to ensure that these programs achieve success.

And as always, we will continue to support the efforts of the National Infrastructure Protection Center and the President's Council on Year 2000 Conversion. I have established close personal relations with Messrs. Vatis, Koskinen and their staffs and we regularly keep each other informed on matters pertaining to our respective responsibilities.

My staff and I are ready to build upon the good work that has been done by our predecessors and look forward to reporting back to you on the success of our endeavors. I thank you again for the invitation and allowing me to present to you my vision for Fiscal Year 2000, and I look forward to your questions.

CIAO Foundations (included for written statement, but not used in oral presentation)

The Critical Infrastructure Assurance Office was created in response to Presidential Decision Directive 63 (PDD-63) as a mechanism to assist in the coordination of the Federal Government's initiatives on critical infrastructure protection. PDD-63 assigned the following specific missions to the CIAO:

* integrating the various infrastructure sector plans into a national plan;

* coordinating departmental analyses on how to mitigate unacceptable risks resulting from the U.S. Government's own dependencies on critical infrastructure;

* coordinating a national education and awareness program targeted toward increasing public understanding and participation in protection efforts; and

* coordinating legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors.

The National Plan for Information Systems Protection-Public-Private Cooperation

The CIAO is working diligently to fulfill its responsibilities under PDD-63. Of primary and immediate significance is completion of the first version of the National Plan for Information Systems Protection. This National Plan addresses, for the first time in our Nation's history, the complex interagency process for approaching critical infrastructure and cyber-related issues. These include, but are not limited to, law enforcement, defense, intelligence, procurement, information technology, and privacy matters. Development and implementation of the National Plan will depend on the continued diligence of a broad array of Federal Government agencies and departments, which must serve as a model for sound cyber security practices and critical infrastructure protection.

As you know, efforts to coordinate a partnership with the private sector are part of the CIAO's mission. The CIAO has carefully engaged the various infrastructure sectors to begin the lengthy process of developing trust, creating new channels of communication, and improving overall cyber security practices.

In implementing its mandates, the CIAO has focused on issues that cut across the responsibilities of multiple departments and agencies, in order to help ensure a coherent and cohesive U.S. approach to the challenges of achieving the protection of our Nation's critical infrastructures.